

(51) Int.Cl. ⁷	識別記号	F I	テロド ⁷ (参考)
G 0 6 F 13/00	3 5 3	G 0 6 F 13/00	3 5 3 C 5 B 0 8 5
	3 5 1		3 5 1 Z 5 B 0 8 9
15/00	3 1 0	15/00	3 1 0 D 5 K 0 3 0
H 0 4 L 12/66		H 0 4 L 11/20	B

審査請求 未請求 請求項の数 2 OL (全 9 頁)

(21) 出願番号 特開2000-177093(P2000-177093)

(22) 出願日 平成12年6月13日 (2000.6.13)

(71) 出願人 500116850

センチュリー・システムズ株式会社

東京都武蔵野市境1丁目15番14号 六ツビル4階

(72) 発明者 下山 智明

東京都武蔵野市境1丁目15番14号 センチュリー・システムズ株式会社内

(74) 代理人 100079108

弁護士 橋本 良幸 (外2名)

Fターム(参考) 5B085 A01 B00 B07

5B089 CA11 GA19 GA21 BA10 KA17

KB13

5B030 GA04 GA08 HA08 BC01 HC13

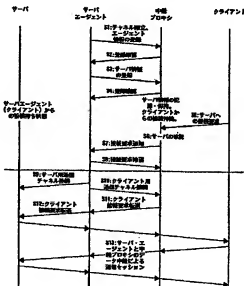
HD01 HD08 HD09 JA11

(54) 【発明の名称】 ネットワークシステム

(57) 【要約】

【課題】 ファイヤーウォールの内側にあるサーバに対して、このファイヤーウォールの外側にあるクライアントからアクセスすることを可能にする。

【解決手段】 ファイヤーウォールの内側にサーバエージェント2を備え、ファイヤーウォールの外側にクライアント4とサーバエージェント2との接続を中継する中継プロキシ1を備えている。サーバエージェント2から中継プロキシ1に対して第1の通信チャネル61を確立し、クライアント4から中継プロキシ1に対して第2の通信チャネル62を確立し (S5)、中継プロキシ1は、クライアント4からのアクセスの情報をサーバエージェント2に通知し (S7)、サーバエージェント2は、サーバ3に対するアクセスの可能な通信チャネルである第3の通信チャネル63を中継プロキシ1との間で確立し (S10)、中継プロキシ1は、第2の通信チャネル62と第3の通信チャネル63とを接続する (S11)。



【特許請求の範囲】

【請求項1】ファイアーウォールの内側またはプライベートアドレス空間にあるサーバに対して、前記ファイアーウォールまたは前記プライベートアドレス空間の外側にあるクライアントからアクセスすることを可能にするシステムであって、

前記ファイアーウォールの内側または前記プライベートアドレス空間にサーバエージェントを備え、

前記ファイアーウォールまたは前記プライベートアドレス空間の外側に、前記クライアントと前記サーバエージェントとの接続を中継する中継プロキシを備え、

前記サーバエージェントから前記中継プロキシに対して第1の通信チャネルを確立し、

前記クライアントから前記中継プロキシに対して第2の通信チャネルを確立し、

前記中継プロキシは、前記クライアントからのアクセスの情報を前記第1の通信チャネルを通じて前記サーバエージェントに通知し、

前記サーバエージェントは、前記サーバに対するアクセスの可能な通信チャネルである第3の通信チャネルを前記中継プロキシとの間で確立し、

前記中継プロキシは、前記第2の通信チャネルと前記第3の通信チャネルとを接続し、

前記中継プロキシおよび前記サーバエージェントを介して前記クライアントと前記サーバの間で通信することを特徴とする、システム。

【請求項2】ファイアーウォールの内側またはプライベートアドレス空間にあるサーバに対して前記ファイアーウォールまたは前記プライベートアドレス空間の外側にあるクライアントからアクセスすることを可能にするため、前記ファイアーウォールまたは前記プライベートアドレス空間の外側に設けられ、

前記ファイアーウォールの内側または前記プライベートアドレス空間に備えられたサーバエージェントからのアクセスを受け付けて第1の通信チャネルを確立し、

前記サーバエージェントに対し、前記第1の通信チャネルを通じて特定要求を送信し、

前記クライアントからのアクセスを受け付けて第2の通信チャネルを確立し、前記クライアントからのアクセスの情報を前記サーバエージェントに対して前記第1の通信チャネルを通じて送信し、

前記サーバエージェントから、前記サーバに対するアクセスの可能な通信チャネルである第3の通信チャネルに関する情報を受信するとともに、前記サーバエージェントとの間に前記第3の通信チャネルを確立し、

前記第2の通信チャネルと前記第3の通信チャネルとを接続する中継プロキシであって、

前記特定要求として、前記クライアントからのアクセスの情報を前記中継プロキシから受信したときは、前記第3の通信チャネルを決定してこれに関する情報を前記中

継プロキシに送信することを前記サーバエージェントに対して要求する、中継プロキシ。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はネットワークシステムに関し、特に、ファイアーウォールの内側またはプライベートアドレス空間にあるサーバに対して、前記ファイアーウォールまたは前記プライベートアドレス空間の外側にあるクライアントからアクセスすることを可能にするシステム、及びそのための中継プロキシに関する。

【0002】

【従来の技術】近年、インターネットが急速な発達を見せている。インターネットを通じてアクセスされるコンピュータやネットワーク機器等のネットワークエレメントは、それぞれ固有のIPアドレスを有し、世界中のどこからでも、そのIPアドレス（グローバルIPアドレス）を指定すれば、インターネットを通じて特定のネットワークエレメントにアクセスすることができる。

【0003】従来から使われているIPアドレス（IPv4バージョン4）は32ビットからなっているため、理論上、約40億通りのIPアドレスを設けることが可能である。しかし、インターネットが予想外の発達を見た結果、近い将来それだけではIPアドレスが足りなくなるといふ問題が叫ばれている（IPアドレス枯渇問題）。

【0004】ところで、上記グローバルIPアドレスを有しないネットワークエレメントをインターネットに接続させる方法として、PAT（Port Address Translation）と呼ばれるアドレス変換機を用いる方法がある。上記グローバルIPアドレスを有しない（プライベートなIPアドレスだけを有している）ネットワークエレメントは、このアドレス変換機を介してインターネットに接続される。上記グローバルアドレスを有しないネットワークエレメントからアドレス変換機に対し、インターネットへの接続を要求すると、アドレス変換機は、当該ネットワークエレメントへのレスポンスを可変とする仮のポート番号を決定し、アドレス変換機自身のグローバルIPアドレスとポート番号を使ってインターネットに接続する。そして、アドレス変換機は、上記仮のポート番号と接続元のネットワークエレメントが持っているIPアドレス（プライベートIPアドレス）との対応関係を一時的に記憶する。

【0005】インターネット上の接続先ネットワークエレメントは、上記の仮のポート番号とアドレス変換機のIPアドレスを指定してレスポンスを送信することにより、アドレス変換機を介して上記の接続元ネットワークエレメントに返信することができる。この方法によればグローバルアドレスを有しないネットワークエレメントがインターネット上のネットワークエレメントに対してアクセスし、接続先のネットワークエレメントからも返

信を行うことができるが、その通信が終了すれば、上記ポート番号とプライベートIPアドレスの対応関係は解除される。従って、インターネット上のネットワークエレメントからプライベートアドレス空間にあるネットワークエレメントに対してアクセスすることはできない。アドレス変換機は、このように外部からのアクセスを制限しているため、ファイアーウォールとして機能することもできる。

【0006】 現行のIPバージョン4による前記IPアドレス枯渇問題を回避するために次世代以降のIPアドレスには32ビットより多くのアドレス空間を割当て、IPバージョン6では128ビットを確保している。しかし、いくらアドレス空間を広げても、限界は存在するので将来上記と同様なアドレス変換機が必要とされる可能性もある。また、IPバージョン6の様に莫大なアドレス空間を持っていたとしても、管理の都合上、一箇まりの複数のネットワークエレメントを一つのIPアドレスで運用する等の目的により、アドレス変換機は使われ続ける。

【0007】 ファイアーウォールの内側にアクセスする方法として、特開平10-285216号に記載のもの知られている。この例では、クライアント終端プロキシとサーバ終端プロキシがそれぞれ中間プロキシに接続することにより、クライアントとサーバとの間に終端間接続をすることができ。

【0008】

【発明が解決しようとする課題】 しかし、上記特開平10-285216号の方法では、クライアント終端プロキシとサーバ終端プロキシの何れか一方が中間プロキシに対して接続した後、他方が中間プロキシに対して接続するまでは、上記一方の接続を維持していなければならない。従って、実際にクライアントとサーバ間での通信が実現する前であっても、クライアントへのアクセスが可能な仮のポート番号を確保しておく必要がある。

【0009】 本発明は、ファイアーウォール又はプライベートアドレス空間の外側からファイアーウォールの内側又はプライベートアドレス空間内のネットワークエレメントにアクセスするに際し、アクセス先であるファイアーウォール等の内側のネットワークエレメントにアクセスするための仮のポート番号を、接続時にのみ確保すれば済むようにするシステムを提供することを目的とする。

【0010】 また、中継プロキシについても、クライアント側に常時接続を確立しておく必要をなくし、更には1つのファイアーウォールの内側に複数のサーバが存在する場合でも、常時各サーバごとに接続を確立しておく必要をなくし、これによってファイアーウォールと中継プロキシのポート番号、メモリ等の資源を有効に利用できることを目的とする。

【0011】 また、ファイアーウォールの外側からアク

セスするに際し、ファイアーウォールやサーバおよびクライアントに対して特別な構成や機能を付加する必要のないシステムを提供することを目的とする。

【0012】

【課題を解決するための手段】 上記の課題を達成するため、本発明のシステムは、ファイアーウォールの内側またはプライベートアドレス空間にあるサーバに対して、前記ファイアーウォールまたは前記プライベートアドレス空間の外側にあるクライアントからアクセスすることを可能にするシステムであって、前記ファイアーウォールの内側または前記プライベートアドレス空間にサーバエージェントを備え、前記ファイアーウォールまたは前記プライベートアドレス空間の外側に、前記クライアントと前記サーバエージェントとの接続を中継する中継プロキシを備え、前記サーバエージェントから前記中継プロキシに対して第1の通信チャネルを確立し、前記クライアントからの前記中継プロキシに対して第2の通信チャネルを確立し、前記中継プロキシは、前記クライアントからのアクセスの情報を前記第1の通信チャネルを通じて前記サーバエージェントに通知し、前記サーバエージェントは、前記サーバに対するアクセスの可能な通信チャネルである第3の通信チャネルを前記中継プロキシとの間で確立し、前記中継プロキシは、前記第2の通信チャネルと前記第3の通信チャネルとを接続し、前記中継プロキシおよび前記サーバエージェントを介して前記クライアントと前記サーバの間で通信することを特徴とする。

【0013】 また、本発明の中継プロキシは、ファイアーウォールの内側またはプライベートアドレス空間の外側にあるサーバに対して前記ファイアーウォールのまたは前記プライベートアドレス空間の外側にあるクライアントからアクセスすることを可能にするため、前記ファイアーウォールまたは前記プライベートアドレス空間の外側に設けられ、前記ファイアーウォールの内側または前記プライベートアドレス空間に備えられたサーバエージェントからのアクセスを受け付けて第1の通信チャネルを確立し、前記サーバエージェントに對し、前記第1の通信チャネルを通じて特定要求を送信し、前記クライアントからのアクセスを受け付けて第2の通信チャネルを確立し、前記クライアントからのアクセスの情報を前記サーバエージェントに対して前記第1の通信チャネルを通じて送信し、前記サーバエージェントから、前記サーバに対するアクセスの可能な通信チャネルである第3の通信チャネルに関する情報を受信するとともに、前記サーバエージェントとの間に前記第3の通信チャネルを確立し、前記第2の通信チャネルと前記第3の通信チャネルとを接続する中継プロキシであって、前記特定要求として、前記クライアントからのアクセスの情報を前記中継プロキシから受信したときは、前記第3の通信チャネルを決定してこれに関する情報を前記中継プロキシに

送信することを前記サーバエージェントに対して要求する。

【0014】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照して説明する。

【0015】（ネットワーク構成）図1は、本発明の一実施形態によるシステムのネットワーク構成を示す図である。このシステムのネットワークエレメントであるサーバ3、サーバエージェント2、中継プロキシ1、クライアント4は、いずれもコンピュータまたは通信装置からなっている。各ネットワークエレメントは通信機能を有している。中継プロキシ1は本発明に特徴的な各種能（後述）を有する。

【0016】中継プロキシ1及びクライアント4は、ネットワーク5に接続されている。ネットワーク5は、典型的にはインターネットが挙げられる。サーバ3及びサーバエージェント2は、ネットワーク5には直接接続されておらず、ファイアウォール7を介してネットワーク5に接続可能になっている。このファイアウォールにより、ファイアウォール内部のサーバ3及びサーバエージェント2に対するファイアウォール外部（クライアント4など）からのアクセスが制限されている。

【0017】サーバ3の符号33、サーバエージェント2の符号21、22、23、中継プロキシ1の符号11、12、13、クライアント4の符号43は、各ネットワークエレメントが他のネットワークエレメントとの通信を行うポートである。なお、サーバ3のポート33は、ネットワーク5には直接接続することができない。

【0018】（接続処理）図2は、上記実施形態によるシステムにおいてクライアントがサーバにアクセスする際の各ポートの接続状況を概念的に示したものである。図中の符号5及び7は、それぞれ図1におけるネットワーク5及びファイアウォール7に相当しており、必ずしもネットワーク5及びファイアウォール7が複数に分断していることを意味しているわけではない。

【0019】図3は、上記実施形態によるシステムにおける接続時の通信シーケンスを示す図である。このシステムでは、以下に詳述するように、サーバ3、サーバエージェント2、中継プロキシ1、クライアント4のそれぞれの間で通信が行われる。

【0020】ステップS1

サーバエージェント2は中継プロキシ1にアクセスし、両者の間に制御用の通信チャネルを確立する。具体的には、図2に示す中継プロキシ上のポート11と、サーバエージェント上のポート21との間に第1の通信チャネル61が確立される。この通信チャネル61は、本システムを利用する間恒久的に維持されることが望ましいが、少なくとも後述のステップS8の処理が実行されるまで維持される。

【0021】また、サーバエージェント2は、中継プロ

キシ1に対してサーバエージェントの情報を送信する。具体的には、サーバエージェントIDと、サーバエージェントが中継プロキシにアクセスするためのパスワードとを送信する。

【0022】ステップS2

中継プロキシ1は、サーバエージェント2から上記サーバエージェントの情報を受信すると、当該サーバエージェントの情報を記憶・保持するとともに、サーバエージェント2に対して上記サーバエージェント情報の登録確認を送信する。

【0023】ステップS3

サーバエージェント2は、中継プロキシ1に対し、サーバ3の情報を送信する。具体的には、ファイアウォール外のネットワークエレメント（中継プロキシ1など）がサーバ3への接続をサーバエージェント2に要求するための接続IDを送信する。

【0024】なお、ステップS3の処理に先立ち、サーバ3からサーバエージェント2にアクセスし、サーバエージェント2が中継プロキシ1にサーバの上記情報を送信するように、サーバ3からサーバエージェント2に依頼するようにしても良い。または管理者によりサーバの上記情報をサーバエージェント2に予め設定するようにしても良い。

【0025】ステップS4

中継プロキシ1は、サーバエージェント2から上記サーバの情報を受信すると、当該サーバの情報を記憶・保持するとともに、サーバエージェント2に対し、サーバの登録確認を送信する。また、中継プロキシ1は、サーバエージェント2に対して特定要求を送信する。特定要求とは、クライアントからの接続要求があったことを送信（後述のステップS7）したときは、サーバへのアクセスが可能な通信チャネルの情報を返信（後述のステップS10）することを要求するものである。

【0026】中継プロキシ1は、上記の送信を行った後、クライアントからの接続待ちの状態となる。

【0027】ステップS5

クライアント4は、中継プロキシ1に対し、サーバへの接続要求を送信する。一般的にはこの接続要求には、サーバの具体的な指定が含まれるが、接続要求にサーバの具体的な指定が含まれない場合には、中継プロキシ1はクライアント4へサーバの具体的な情報を問合せすることもある。

【0028】ステップS6

中継プロキシ1は、サーバへの上記接続要求をクライアント4から受信すると、該当するサーバが存在するかどうかを判断する。また、クライアント4から受信したサーバへの上記接続要求を、後述のステップS11まで保持する。

【0029】なお、ここで、クライアント4と中継プロキシ1との通信チャネルである第2の通信チャネル62

が確立される。

【0030】ステップS7

中継プロキシ1は、サーバエージェント2に対し、サーバへの上記接続要求がクライアントからあったことを、サーバへの接続が許可されるために上記ステップS3で設定された接続ID等の情報を使って通知する。

【0031】ステップS8

サーバエージェント2は、中継プロキシ1からの上記通知を受信すると、上記ステップS7で通知された接続IDが、上記ステップS3で設定された接続IDと一致するか否かを判断する。接続IDが一致した場合には、この通知の受信確認を中継プロキシ1に対して送信する。

【0032】ここまでの中継プロキシ1とサーバエージェント2との間の通信は、第1の通信チャネル61を通じて行われる。

【0033】ステップS9

サーバエージェント2は、サーバ3との間で通信チャネルを確立する。具体的には、図2に示すサーバエージェント上のポート23と、サーバ上のポート33との間に通信チャネル64（第4の通信チャネル）を確立する。

【0034】ステップS10

サーバエージェント2は、中継プロキシ1との間で、上記サーバに接続するための通信チャネル（第3の通信チャネル63）を確立する。具体的には、サーバエージェント上のポート22から、中継プロキシ1上の任意のポート（例えばポート12）に対してアクセスして通信チャネルを確立する。

【0035】更にサーバエージェント2は、中継プロキシ1との間に確立された上記第3の通信チャネル63と、上記ステップS9でサーバ3との間に確立された第4の通信チャネル64とを接続する。言い換えれば、サーバエージェント2上のポート22とポート23とを互いに接続し、ポート22に入った情報がポート23に送られるようにし、逆にポート23に入った情報がポート22に送られるようにする。

【0036】ステップS11

中継プロキシ1は、サーバエージェント2からのアクセスを受けて第3の通信チャネル63が確立されると、この第3の通信チャネル63と、クライアント4との間に確立された第2の通信チャネル62とを接続する。言い換えれば、中継プロキシ1上のポート12とポート13とを互いに接続し、ポート12に入った情報がポート13に送られるようにし、逆にポート13に入った情報がポート12に送られるようにする。

【0037】この結果、上記ステップS5においてクライアント4から送信され中継プロキシ1に保持されていたサーバへの接続要求が、第3の通信チャネル63を通じてサーバエージェント2に転送される。

【0038】ステップS12

サーバエージェント2は、中継プロキシ1から転送され

てきたクライアントからサーバへの接続要求を、第4の通信チャネル64を通じてサーバ3に転送する。

【0039】ステップS13

以後、サーバ3～第4の通信チャネル64～サーバエージェント2～第3の通信チャネル63～中継プロキシ1～第2の通信チャネル62～クライアント4、又はその逆という通信経路によって、サーバ3とクライアント4との間で相互に通信を行うことが可能となる。サーバ3とクライアント4は、この時点でアクセス権限確認のための認証手続きを再度行ってもよい。

【0040】（終了処理）図4は、この実施形態のシステムにおいて確立されたサーバ3とクライアント4との間の接続を終了するための通信シーケンスを示す図である。

【0041】ステップS14

クライアント4は、サーバ3に対し、中継プロキシ1およびサーバエージェント2を経由して通信の切断要求を送信する。

【0042】ステップS15

サーバ3は、クライアント4からの上記切断要求を受信すると、サーバエージェント2との間の第4の通信チャネル64を切断する。

【0043】ステップS16

サーバエージェント2は上記通信チャネル64の切断を検知し、中継プロキシ1との間の第3の通信チャネル63を切断する。

【0044】ステップS17

中継プロキシ1は上記第3の通信チャネル63の切断を検知し、クライアント4との間の第2の通信チャネル62を切断して一連の処理が終了する。

【0045】なお、ここでは、終了処理がクライアント4からの切断要求によってサーバ側から切断が開始されたが、これに限らず、サーバ3からの切断要求によって開始できるようにしてもよい。

【0046】また、切断要求を待たず、サーバ3またはクライアント4から切断を開始するようにしてもよい。図6は切断要求を待たず、クライアント4から切断を開始して接続を終了する組合の通信シーケンスである。図に示されるように、上記ステップS13における通信セッションの後、ステップS18において、クライアント4が中継プロキシ1との間の通信チャネル（第2の通信チャネル62）を切断する。次にステップS19において、中継プロキシ1は、第2の通信チャネル62の切断を検知すると、サーバエージェント2との間の通信チャネル（第3の通信チャネル63）を切断する。最後にステップS20において、サーバエージェント2は、第3の通信チャネル63の切断を検知すると、サーバとの間の第4の通信チャネル64を切断して一連の処理を終了する。

【0047】（本実施形態による利点）本実施形態で

は、以上のように、ステップS5においてクライアント4からのアクセスがあって初めて、ステップS10においてサーバ3ないしサーバエージェント2との通信チャネル(第3の通信チャネル63)が確立されるようになっている。このため、第3の通信チャネル63のためにサーバエージェント2に用意されるポート22は、クライアント4からのアクセスがあった後で決定すれば良い。従って、ポート22を占有する時間は通信が実際に行われている間だけでよく、ポートの占有時間が短くて済む。従って、ファイアーウォール内に複数のサーバを配置した場合には、サーバエージェント上のポート22がサーバ3との通信に占有されていないれば、他のサーバが使うことができる。また、ポート22が使用中であっても別のポートを新たに割当て同様に通信することができる。また、常時確保しておく通信チャネルは第1の通信チャネル61のみでよく、サーバに接続するための通信チャネルを各サーバごとに用意しておく必要はない。

【0048】また、本実施形態では、サーバ3とクライアント4に対して特別な構成又は機能を付加する必要がなく、中継プロキシ1とサーバエージェント2を設置するだけで、ファイアーウォールの外側からアクセスすることを可能にするシステムを実現することができる。このシステムは、サーバ3、サーバエージェント2、クライアント4が複数存在している1台の中継プロキシで実現することができる。

【0049】また、このシステムは、サーバエージェント2と中継プロキシ1との間に、ファイアーウォール7が多段階に構成されていても実現することができ、中継プロキシ1とクライアント4との間にファイアーウォールが構成されていても実現することができる。

【0050】(他の実施形態) 以上説明した実施形態では、サーバ3及びサーバエージェント2はファイアーウォール7の内側にあるものとして説明したが、これに限らず、アドレス変換機によってグローバルアドレス空間と隔てられたプライベートアドレス空間にある場合でも、本発明を適用することができる。

【0051】また、サーバエージェント2は、サーバ3

と同一のマシン内にソフトウェアとして実現されることもできる。この場合でも、第1の通信チャネル61及び第3の通信チャネル63は中継プロキシとサーバエージェントのプログラムとの間に確立され、第4の通信チャネル64はサーバエージェントのプログラムとサーバのプログラムとの間に確立される。

【0052】

【発明の効果】以上説明したように、本発明によれば、ファイアーウォールの外側からアクセスするに際し、アクセス先であるファイアーウォール内のネットワークエレメントにアクセスするための仮のポート番号を、接続時にのみ確保すれば済むようにするシステムを提供することができる。

【0053】また、中継プロキシも、クライアント側に常時接続を確立しておく必要がなく、更には1つのファイアーウォールの内側に複数のサーバが存在する場合でも、常時各サーバごとに接続を確立しておく必要がないため、中継プロキシのポート番号、メモリ等の資源を有効に利用することができる。

【0054】また、ファイアーウォールの外側からアクセスするに際し、ファイアーウォールやクライアントに対して特別な構成や機能を付加する必要のないシステムを提供することができる。

【図面の簡単な説明】

【図1】 本発明の一実施形態によるシステムのネットワーク構成を示す図である。

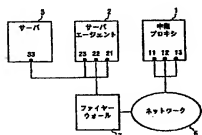
【図2】 上記実施形態によるシステムにおいてクライアントがサーバにアクセスする際の各ポートの接続状況を概念的に示したものである。

【図3】 上記実施形態によるシステムにおける接続時の通信シーケンスを示す図である。

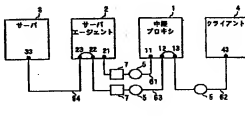
【図4】 この実施形態のシステムにおいて確立されたサーバとクライアントとの間の接続を終了するための通信シーケンスを示す図である。

【図5】 切断要求を待たず、クライアント4から切断を開始して接続を終了する場合の通信シーケンスを示す図である。

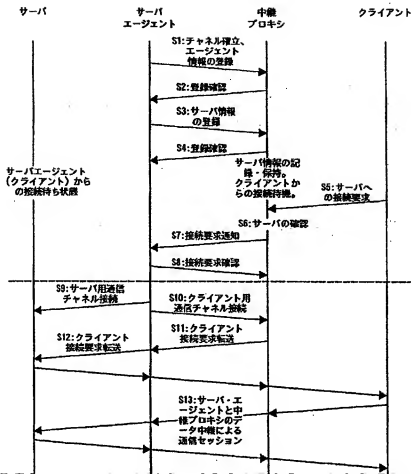
【図1】



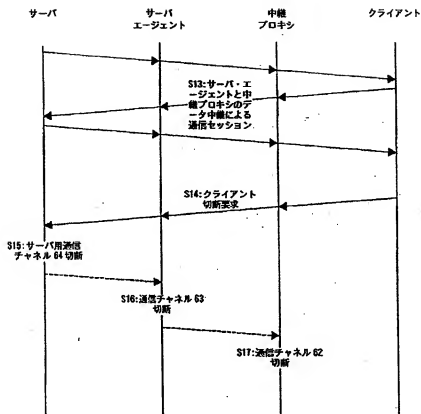
【図2】



【図3】



【図4】



【図5】

